Правительство Ростовской области

Управление государственной службы занятости населения Ростовской области (УГСЗН Ростовской области)

ПОСТАНОВЛЕНИЕ

31 мая 2017 г. № 4

г. Ростов-на-Дону

Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных управления государственной службы занятости населения Ростовской области

В соответствии с Федеральным законом от 27.07.2006 № 152 - ФЗ «О персональных данных» управление государственной службы занятости населения Ростовской области **п о с т а н о в л я е т :**

1. Определить угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных управления государственной службы занятости населения Ростовской области, согласно приложению.

2. Рекомендовать государственным казенным учреждениям Ростовской области центрам занятости населения, руководствоваться настоящим постановлением при определении угроз безопасности персональных данных, актуальных при обработке персональных данных в используемых ими информационных системах персональных данных.

3. Настоящее постановление вступает в силу со дня его официального опубликования.

4. Контроль за выполнением настоящего постановления оставляю за собой.

Начальник управления С.Р. Григорян

Приложение
к постановлению УГСЗН
Ростовской области
от 31 мая 2017 г. № 4

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных управления государственной службы занятости населения Ростовской области

1. Угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы по техническому и экспортному контролю Российской Федерации:

1.1. Просмотр информации на дисплее пользователей информационной системы персональных данных (далее – ИСПДн) работниками, не допущенными к персональным данным (далее – ПДн);

1.2. Просмотр информации на дисплее пользователей ИСПДн посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн;

1.3. Перехват управления загрузкой операционной системы (ОС) ИСПДн, в том числе с использованием отчуждаемых носителей информации, и получение прав доверенного пользователя для осуществления несанкционированного доступа (далее – НСД) к ПДн;

1.4. Вызов штатных программ ОС ИСПДн или запуск специально разработанных программ, реализующих НСД к ИСПДн;

1.5. Перехват и анализ сетевого трафика для извлечения конфиденциальной или аутентификационной информации;

1.6. Сканирование сети для выявления используемых протоколов, доступных портов сетевых служб, закономерностей формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей;

1.7. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;

1.8. Навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

1.9. Внедрение ложного объекта сети;

1.10. Сетевые атаки типа «Отказ в обслуживании»;

1.11. Удаленный запуск приложения в ИСПДн;

1.12. Внедрение по сети вредоносных программ;

1.13. Хищение элементов ИСПДн, содержащих ПДн;

1.14. Вывод из строя элементов ИСПДн;

1.15. Внедрение в ИСПДн аппаратных закладок;

1.16. Утрата паролей доступа к ИСПДн;

1.17. Выход из строя аппаратно-программных средств ИСПДн;

1.18. Угроза автоматического распространения вредоносного кода в грид-системе;

1.19. Угроза внедрения вредоносного кода в BIOS;

1.20. Угроза внедрения кода или данных;

1.21. Угроза восстановления предыдущей уязвимой версии BIOS;

1.22. Угроза деструктивного изменения конфигурации/среды окружения программ;

1.23. Угроза загрузки нештатной операционной системы;

1.24. Угроза изменения системных и глобальных переменных;

1.25. Угроза использования информации идентификации/аутентификации, заданной по умолчанию;

1.26. Угроза межсайтового скриптинга;

1.27. Угроза межсайтовой подделки запроса;

1.28. Угроза нарушения изоляции среды исполнения BIOS;

1.29. Угроза невозможности управления правами пользователей BIOS;

1.30. Угроза некорректного использования функционала программного обеспечения;

1.31. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS;

1.32. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети;

1.33. Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы;

1.34. Угроза несанкционированного использования привилегированных функций BIOS;

1.35. Угроза несанкционированного редактирования реестра;

1.36. Угроза несанкционированного создания учетной записи пользователя;

1.37. Угроза несанкционированного удаленного внеполосного доступа к аппаратным средствам;

1.38. Угроза несанкционированного управления указателями;

1.39. Угроза обхода некорректно настроенных механизмов аутентификации;

1.40. Угроза удаления аутентификационной информации;

1.41. Угроза установки уязвимых версий обновления программного обеспечения BIOS;

1.42. Угроза эксплуатации цифровой подписи программного кода;

1.43. Угроза включения в проект недостоверно испытанных компонентов;

1.44. Угроза заражения компьютера при посещении неблагонадежных сайтов;

1.45. Угроза наличия механизмов разработчика;

1.46. Угроза распространения «почтовых червей»;

1.47. Угроза несанкционированного использования системных и сетевых утилит.

2. Угрозы безопасности персональных данных, определяемые согласно требованиям Федеральной службы безопасности Российской Федерации:

2.1. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны;

2.2. Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы средства криптографической защиты информации (далее – СКЗИ) и среда их функционирования (далее – СФ);

2.3. Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:

сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы;

сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы;

сведений о мерах по разграничению доступа в помещения, в которых находятся средства вычислительной техники, на которых реализованы СКЗИ и СФ.

Начальник отдела
организационно-кадровой
работы и делопроизводства  А.М. Оленников